NIST National Institute of Standards and Technology • U.S. Department of Commerce
INFORMATION TECHNOLOGY LABORATORY
NO. 100 November 2007

ITL'S RICH PROGRAMMATIC DIVERSITY

NIST's Information Technology Laboratory promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology through research and development in information technology, mathematics, and statistics. To accomplish this mission, ITL organizes its research into nine broad programs:

Complex Systems: Complex Systems are composed of large interrelated, interacting entities which taken together, exhibit a macroscopic behavior which is not predictable by examination of the individual entities. The Complex Systems Program seeks to understand the fundamental science of these systems and develop rigorous descriptions (analytic, statistical, or semantic) that enable prediction and control of their behavior. Initially focused on the Internet and Grid Computing, this Program will facilitate predictability and reliability in these areas and other complex systems such as biotechnology, nanotechnology, semiconductors, and complex engineering**.** Sandy Ressler is the Program Manager.

Cybersecurity: Cybersecurity is focused on ensuring three security objectives of information technology systems: confidentiality, integrity, and availability. The Cybersecurity Program creates a balance between our statutory responsibilities and a basic and applied research program. The Program addresses long-term scientific issues in some of the building blocks of IT security - cryptography, security testing and evaluation, security metrics, and security properties - providing a more scientific foundation for cybersecurity, while maintaining a focus on near-term issues in IT system security. The Program Manager is Tim Grance.

Enabling Scientific Discovery: Modern scientific research has become more and more dependent on mathematical, statistical, and computational tools for enabling discovery. The Enabling Scientific Discovery Program promotes the use of these tools to dramatically advance our ability to predict the behavior of a broad range of complex scientific and engineering systems and enhance our ability to explore fundamental scientific processes. This Program focuses on inter-disciplinary scientific projects that involve novel computational statistics and the development of simulation methods and software. These efforts will have a foundational impact on scientific discovery throughout U.S. industry, government, and academia. Tony Kearsley is the Program Manager.

Identity Management Systems: Identity management systems are responsible for the creation, use, and termination of electronic identities which are routinely used to access logical and physical resources, and have become a ubiquitous part of our national infrastructure. The Identity Management Systems Program is pursuing the development of common models and metrics for identity management, critical standards, and interoperability of electronic identities. These efforts will improve the quality, usability, and consistency of identity management systems while protecting privacy. The Program Manager is Jim Dray.

Information Discovery, Use, and Sharing: Society is awash in data - our ability to amass data has outpaced our ability to use it. Extracting knowledge, information, and relationships from this data is one of the greatest challenges faced by the scientists in the twenty-first century. The data can be as diverse as biological research data, medical images, automated newswire, speech, or video. The Information Discovery, Use, and Sharing Program fosters innovation throughout the information life cycle by developing the measurement infrastructure to enhance knowledge discovery, information exchange, and information usability. The Program enables novel computational approaches to data collection and analysis to be combined with improved interoperability techniques to effectively extract needed information from the wealth of available data. Mary Brady is the Program Manager.

Pervasive Information Technologies: Pervasive information technology is the trend towards increasingly ubiquitous connected computing sensors, devices, and networks that monitor and respond transparently to human needs. The Pervasive Information Technologies Program facilitates the creation of standards for sensor communication, networking interoperability, and sensor information security. The Program enables the use of pervasive information technologies to enhance personal and professional productivity and quality of life. The Program Manager is Kamran Sayrafian.

Trustworthy Networking: The Trustworthy Networking Program's research encompasses the security, reliability, scalability, robustness, adaptability, and performance of networking technologies. The Program includes long-term fundamental research that is vetted against existing networking protocols. These efforts provide commercially viable techniques to test, measure, and improve the trustworthiness of networking technologies at the earliest

INFORMATION TECHNOLOGY LABORATORY

If you are interested in receiving our newsletter, send your name, organization, and business mailing address to:

ITL Newsletter
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900

You will be placed on this mailing list only.

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of new information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov.

ITL Editor: Elizabeth B. Lennon
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900
Phone: (301) 975-2832
Fax: (301) 975-2378
E-mail: elizabeth.lennon@nist.gov

stages of development. Tom Karygiannis is the Program Manager.

Trustworthy Software: Trustworthy software is software that performs as intended for a specific purpose, when needed, with operational resiliency and without unwanted side effects, behaviors, or exploitable vulnerabilities. The Trustworthy Software Program will improve the ability to model, produce, measure, and assess trustworthiness in software through new and innovative technologies, models, measurement methods, and software tools. The resulting technologies, models, methods, and tools will reduce the cost and time of building in or assessing software trustworthiness in applications and systems. The Program Manager is Tom Rhodes.

Virtual Measurement Systems: A virtual measurement is a quantitative result and its uncertainty, obtained primarily by a nontrivial computer simulation or computer-assisted measurements, for example, computational models of physical systems. The Virtual Measurement Systems Program introduces metrology constructs, standard references, uncertainty characterization, and traceability into scientific computation and computer-assisted measurement technologies. Uncertainty characterization and traceability in modeling will result in predictive computing with quantified reliability. Andrew Dienstfrey is the Program Manager.

For more information, go to http://www.itl.nist.gov.

ITL's Work Helps to Improve the Nation's Voting Systems and Processes

At the August plenary meeting of the Technical Guidelines Development Committee (TGDC), the NIST/ITL Voting Standards team presented to the advisory committee the next iteration of the Voluntary Voting System Guidelines (VVSG). The TGDC voted unanimously to adopt the document and delivered it to the U.S. Election Assistance Commission (EAC) on September 4, 2007. Following a public review of the recommendations, the EAC will address comments from the review process prior to approving the guidelines for the nation. The NIST/ITL Voting Standards team provided technical expertise in computer security, human factors, and core requirements for the VVSG; the work was mandated by the Help America Vote Act of 2002. The recommended guidelines are available at http://vote.nist.gov.

FEDERAL INFORMATION PROCESSING STANDARDS (FIPS) ACTIVITIES

ITL Issues Call for New Cryptographic Hash Algorithm (SHA-3)

On November 2, 2007, a Federal Register notice announced a public competition to develop a new cryptographic "hash" algorithm, which converts a variable length message into a short "message digest" that can be used for digital signatures, message authentication, and other applications. The announcement specifies the submission requirements, the minimum acceptability requirements, and the evaluation criteria for candidate hash algorithms. The competition is ITL's response to recent advances in the cryptanalysis of hash functions. The new hash algorithm will be called "SHA-3" and will augment the hash algorithms currently specified in FIPS 180-2, Secure Hash Standard. Entries for the competition must be received by October 31, 2008. Details about the competition are available at *http://www.nist.gov/hash-competition*.

SELECTED NEW PUBLICATIONS

The Fifteenth Text REtrieval Conference (TREC 2006) Proceedings

Ellen Voorhees and Lori Buckland, Editors
NIST Special Publication 500-272
September 2007
http://trec.nist.gov/pubs/trec15/t15_proceedings.html

This document presents the proceedings of the fifteenth Text REtrieval Conference (TREC 2006) held at NIST on November 14-17, 2006. Participants in TREC 2006 included 107 groups from 17 countries. Conference cosponsors included NIST, the Defense Advanced Research Projects Agency (DARPA),

and the Advanced Research and Development Activity (ARDA).

Guide to Secure Web Services
By Anoop Singhal, Theodore Winograd, and Karen Scarfone
NIST Special Publication 800-95
August 2007
http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf

Web services based on open standards and deployed in Service Oriented Architectures allow data and applications to interact without human intervention through dynamic and ad hoc connections. Ensuring the security of Web services involves augmenting traditional security mechanisms with security frameworks based on use of authentication, authorization, confidentiality, and integrity mechanisms. This document describes how to implement those security mechanisms in Web services and discusses how to make Web services and portal applications robust against the attacks to which they are subject.

Cryptographic Algorithms and Key Sizes for Personal Identity Verification (PIV)
By W. Timothy Polk, Donna F. Dodson, and William E. Burr
NIST Special Publication 800-78-1
August 2007
http://csrc.nist.gov/publications/nistpubs/800-78-1/SP-800-78-1_final.pdf

SP 800-78-1 has been modified to enhance interoperability, simplify the development of relying party applications, and enhance alignment with the National Security Agency's *Suite B Cryptography* [SUITE B]. Revision 1 reduces the set of elliptic curves approved for use with PIV cards and the supporting infrastructure from six curves to two. Also, Secure Hash Algorithm (SHA)-384 has been added for use with Curve P-384 in this revision. And finally, this revision eliminates the largest size of RSA keys (3072 bits) on PIV cards.

Maze Hypothesis Development in Assessing Robot Performance during Teleoperation
By Salvatore Schipani and Elena Messina
NISTIR 7443
August 2007
E-mail salvatore.schipani@nist.gov

NIST personnel assessed 14 prospective Urban Search and Rescue robots for the purposes of developing performance standards which currently do not exist. During this exercise, a maze configuration – hypothesized as potentially valid test methodology – was assessed. Among the findings, resultant significant differences in completion and decision-making times facilitated classifying platforms based on performance. Also revealed was the fact that errors in navigation and encounters with walls correlated with times taken in making decisions… the longer it took to make a decision, the greater the chance this decision was incorrect. Results validated the hypothesis of a maze as beneficial in eliciting data necessary for human-controlled robot performance assessment.

Meta-Analysis of Third-Party Evaluations of Iris Recognition
By Elaine Newton and P. Jonathon Phillips
NISTIR 7440
August 2007
http://iris.nist.gov/ice/IrisComparisonY070820_NISTIR.pdf

Iris recognition has long been widely regarded as a highly accurate biometric, despite the lack of independent large-scale testing of its performance. Recently, however, three third-party evaluations of iris recognition were performed. This report compares and contrasts the results of these independent evaluations and finds that despite differences in methods, hardware, and/or software among them, all three studies report error rates of the same order of magnitude, and the differences between the best performers' error rates are an order of magnitude smaller than the errors.

6th Annual PKI R&D Workshop: "Applications-Driven PKI" Proceedings
By William T. Polk and Kent Seamons
NISTIR 7427
September 2007
http://csrc.nist.gov/publications/PubsNISTIRs.html

ITL hosted the sixth Annual Public Key Infrastructure (PKI) Research Workshop on April 17-19, 2007. The event brought together PKI experts from academia, industry, and government who had a particular interest in novel approaches to simplifying the use and management of X.509 digital certificates, both within and across enterprises. This proceedings document includes the nine refereed papers and captures the essence of the keynote, four panels, and interaction at the workshop.

"ITL" Available Via E-Mail
We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send and e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-newsletter**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message HELP. To have the newsletter sent to an e-mail address other than the FROM address, contact the ITL editor.

MARK YOUR CALENDAR

Health Insurance Portability and Accountability Act (HIPAA) Security Rule Implementation and Assurance Workshop
Date: January 16, 2008
Place: NIST, Gaithersburg, Maryland
Sponsors: NIST and Centers for Medicare and Medicaid Services

Targeted toward HIPAA Security Rule implementers, covered entity privacy officers, security officers, compliance

officers, and audit staff, this workshop will focus on challenges, tips, techniques, and issues surrounding implementing, adhering to and auditing HIPAA Security Rule requirements. Topics include NIST Special Publication 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*; automation of security and compliance; standards selection and deployment; threats, vulnerabilities and techniques; and HIPAA assessments.

NIST contacts: Matthew Scholl, 301/975-2941, mscholl@nist.gov
Kevin Stine, 301/975-4483, kstine@nist.gov
Conference website: http://www.nist.gov/public_affairs/confpage/080116.htm

7th Symposium on Identity and Trust on the Internet (IDtrust 2008)
Dates: March 4-6, 2008
Place: NIST, Gaithersburg, Maryland
Sponsors: NIST, Internet 2, Organization for the Advancement of Structured Information Standards (OASIS) and Federal Public Key Infrastructure Policy Authority (FPKIPA)

Theme: Identity and Trust Infrastructures: This symposium will bring together academia, government, and industry to explore all aspects of identity and trust. Previously known as the PKI R&D Workshop (2002-2007), our new name reflects interest in a broader set of tools and the goal of an identity layer for the Internet. We aim to get practitioners in different sectors together to apply the lessons of real-world deployments to the latest research and ideas on the horizon.

NIST contact: Tim Polk, 301/975-3348, william.polk@nist.gov
Conference website: http://middleware.internet2.edu/idtrust

21st Annual Federal Information Systems Security Educators' Association (FISSEA) Conference
Dates: March 11-13, 2008
Place: NIST, Gaithersburg, Maryland
Sponsors: NIST and FISSEA

With a theme of "Security Through Innovation and Collaboration," this year's FISSEA conference will provide dual tracks of high-quality presentations, great networking opportunities, and vendors providing service information. Security awareness, training, and education practitioners can discover new ways to improve their IT security programs. Attendees can gain awareness and training ideas and resources, obtain practical solutions to training problems, and earn Continuing Professional Education (CPE) credits.

NIST contact: Mark Wilson, 301/975-3870, mark.wilson@nist.gov
Conference website: http://csrc.nist.gov/organizations/fissea/2008-conference/

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.